1.0 PURPOSE

The purpose of this policy is to provide guidelines for accessing the Department of Public Safety's Information Technology resources.

2.0 POLICY

It is the policy of the Department of Public Safety to ensure that access to the Department's Information Technology resources are adequately controlled and monitored.

3.0 APPLICABILITY

This policy applies to all authorized users of the Department of Public Safety, including full-time employees, part-time employees, and contractors.

4.0 REFERENCES

A. NMAC 1.12.11.16, Enterprise Architecture

B. NMAC 1.12.10.9, Internet, Intranet, Email, and Digital Network Usage

C. STD006.001, Virus and Malicious Code Standard

D. S-STD007.002, Session Controls Standard

E. S-STD004.001, Account Management Standard

F. S-STD009.001, IT Physical Security

G. FBI CJIS Security Policy v4.2

5.0 DEFINITIONS

A. Access (1) – The ability or right to approach, enter, exit, or communicate with or make use of a resource or an area containing a resource.

B. Access (2) – The process of retrieving data from the network. Access is restricted by permissions that are granted to accounts or groups of accounts to network resources.

C. Account – An object in the network that is used to access resources.

D. Advanced Authentication – An extra layer of security designed to further verify the identity of an account that is trying to access the network. There are several forms of Advanced Authentication defined by the CJIS security policy, any of which, when implemented with regular authentication, provide the required security for accessing the network. Examples include …….These forms are:

1. Virtual Private Networks
2. Biometric Devices

3. Public Key Infrastructure
4. Smart Cards
5. Token Devices

E. Criminal Justice Information System (CJIS) – A division within the United States Federal Bureau of Investigation (FBI) that is responsible for providing timely information to the FBI and other criminal and non-criminal justice agencies and institutions about law enforcement–related matters.

F. Dissemination – The process of distributing data.

G. Encryption – The process of making data unreadable without the corresponding decryption algorithm. This process can be simple obfuscation or can involve highly complex mathematical formulae.

Added. **H. MDC –** Mobile Data Computer.

I. Network – The communication infrastructure that is used to store and transmit data.

J. Network Device – Any device or component that provides access to or controls the communication infrastructure of the network. This includes, but is not limited to, routers, switches, hubs, modems, wireless access points, and remote access devices.

K. Password (Fixed) – A secret set of characters, set by a user, which, in combination with a User ID, grants access to network resources for an account. The policies in this document regarding password changes only apply to fixed (set by a user) passwords and not to system-generated, one-time dynamic passwords.

L. Physically Secure Location – Any area that has controlled and monitored access.

M. Privilege – The rights that are granted to an account to perform certain tasks on the network.

N. Remote Access – The process of accessing the network using a public network. This is usually through dial-up, using the Public Switched Telephone Network (PSTN) or through a Virtual Private Network (VPN) using an encrypted path through the Internet.

O. Resource – Any file, folder, network share point, server, or device that contains data or controls the flow of data on the network.

P. User ID – A unique identifier that differentiates one account from another. User IDs are not secret although they should be treated as sensitive to non-administrative persons.

Q. Wireless Local Area Network (WLAN) – A network that connects computers and resources over a radio frequency. A WLAN can be used to extend the network to areas for temporary access or where running cable is too expensive.

6.0 PROCEDURE

A. Network Access – this section contains all policy requirements regarding the granting and removal of access to the network and resources on the network.

1. All employees and contractors that will have physical and/or network access to Department of Public Safety network resources must pass a fingerprint-based criminal background check. Convictions will be reviewed by CSO (Chief Security Office) and CIO or their designee.

2. All persons that are to have access to DPS network resources shall be uniquely identified by use of a unique identifier (user ID) that represents a user account.

3. Users are responsible for all activity performed with their user IDs. User IDs shall not be utilized by anyone but the individuals to whom they have been issued. Users shall not allow others to perform any activity with their user-IDs. Accounts shall not be shared between users, except for limited-access training labs.

4. All users shall have a single account with the exception of administrative users, who will have an additional elevated privileges account.

5. Elevated-privilege accounts shall be used only for administrative tasks and not for day-to-day operations.

6. No regular user account shall be given permanent administrative privileges on any computer.

7. Access Procedure

   a. Accounts shall be disabled upon termination of an employee's or contractor's employment. Accounts shall be disabled during administrative suspension of employees. After 90 days the account will be deleted.

   b. Access to restricted network information, resources, or devices shall be granted after a written access authorization form is completed for the following circumstances.

      1. New Hire

      2. Change of Job Duties

   c. Security groups that grant or deny access to IT assets shall be completely documented and maintained in a current state by the Chief Security Officer or designee.

   d. All network access shall be revoked for any of the following reasons.

      1. Change of Job Duties

      2. Transfer to Another Agency

      3. Resignation

      4. Termination or Contract Expiration

      5. Alleged Inappropriate Behavior

B. Passwords – This section contains all policy requirements regarding the use and protection of basic authentication passwords.

1. Password Construction

   a. Passwords shall be a minimum of eight (8) characters.

   b. Passwords shall not be any word found in any dictionary in any language or a proper name.

   c. Passwords shall not be the same as the user ID or contain more than two (2) consecutive characters that match any part of the user ID.

d. Passwords shall contain at least three of the following four criteria: uppercase alphabet characters, lowercase alphabet characters, numbers, and special characters.

e. Users shall not construct passwords by combining a set of characters that do not change with a set of characters that predictably change. Example: ABc123, ABc345, ABc678

2. Changing Passwords

a. Passwords shall be changed at least every ninety (90) days.

b. Passwords shall not be changed more frequently than once per three (3) days.

c. Systems shall prevent a password from being changed to a password that has been used in the previous ten (10) passwords.

d. System-level passwords (administrative and service accounts) must be changed at least every six (6) months or if a person with administrative permissions leaves the agency the system-level passwords will be changed immediately.

3. Storing and Disseminating Passwords

a. Unencrypted passwords shall not be displayed or stored in readable format on desks, in drawers, on permanent storage, or in software of any kind.

b. Passwords shall not be sent through unencrypted electronic mail.

4. General Password Security

a. All users requiring network access shall be given a unique user ID and a password.

b. Passwords shall not be shared between users or disclosed to any individual, ever.

c. If a password is forgotten, the account holder's (user's) supervisor will contact the help desk by email. The help desk will contact the user by telephone and give them the new password. The new password shall need to be changed at the first log on by the user.

d. Passwords shall not be re-used by the same user between different accounts, except when special permission is granted.

e. User-created passwords will not be used on encryption utilities.

f. User accounts shall be locked out for thirty (30) minutes after three (3) incorrect passwords are entered in a one (1) minute period.

C. Physical Access

1. Access to physically secure locations

a. Access to areas containing workstations that are not used to access protected data shall be controlled by the site's physical security controls.

b. Access to areas containing workstations that are used to access protected data shall use enhanced physical controls over and above those used to access general workstation areas. Persons that must have access to these areas that should not have access to CJIS data shall be escorted at all times.

c. Access to areas containing servers and/or network devices shall use a different set of controls than are used to gain access to workstation areas, even if the workstation areas are used to access protected data. Persons that must have access to these areas that should not have access to protected data shall be escorted at all times.

d. Access to areas containing MDCs shall be the responsibility of the authorized employee to whom it was issued.

2. Any area containing devices that are used to access or view protected data shall use view-limiting mechanisms to prevent casual viewing of restricted data.

3. Any area that is a physically secured location shall be posted "Authorized Personnel Only" with a sign that measures no less than 12 inches by 12 inches at every access point.

D. Remote Access

1. The DPS network shall only be accessed through approved channels and from approved locations.

2. Remote access shall be granted to users on an as-needed basis using the policy for elevating access (Section A.7.a).

3. All remote access shall use Virtual Private Networks

4. All remote access attempts shall be logged.

5. External agencies or vendors may have remote access to DPS resources if a legitimate need exists and advanced authentication policies are met.

E. WLAN Access

1. All WLAN access shall use a minimum of 128-bit encryption.

2. All WLAN access shall use encrypted authentication.

3. Refer to wireless policies in State of New Mexico ACR N-STD-008.

F. Advanced Authentication

1. All remote computers and networks that communicate with the Department of Public Safety over a public network shall use Virtual Private Networks or SSL.

G. Network Device Access

1. All vendor-supplied default passwords shall be changed before any computer or communications system is used for Department of Public Safety business.

2. All Department of Public Safety network devices shall have unique passwords or other access control mechanisms.

H. Dissemination of Protected Materials

1. Authorized users shall access systems and disseminate data only for the purposes for which they are authorized.

2. No sensitive materials, including classified, Sensitive But Unclassified (SBU), or information which could affect an individual's privacy shall be posted to a public website or otherwise disclosed to the public unless required by law

I. Enforcement

1. Violations of this policy shall be investigated promptly and efficiently by objective and appropriate staff to be designated by the DPS Secretary or his designee.

2. Classified employees suspected of violating this policy shall be given notice of any investigation and an opportunity to present any relevant, exculpatory evidence or mitigating circumstances regarding the charge of the violation. Investigations of alleged violations of this policy involving commissioned personnel will be conducted in accordance with DPS Policy ADM:04, Internal investigations.

3. If the investigation shows the staff member violated this policy, the staff member may be subject to suspension or termination of access to IT resources, as well as disciplinary action up to termination of employment and/or criminal indictment.

J. General Network Use

1. All users will comply with all security policies of the State of New Mexico and the New Mexico Department of Public Safety and shall sign a statement indicating they have received and read all DPS policies and their intent to comply with those policies.

2. Users are responsible for all activity performed with their user IDs.

3. DPS computers, MDC's and other communications systems may be utilized as alternative modes of communication. They shall be used for business purposes only. Incidental personal use is permissible if the use:

   a. Does not consume more than a trivial amount of resources that could otherwise be used for business purposes, and

   b. Does not interfere with worker productivity

   c. Unacceptable personal use of DPS IT resources include soliciting business, selling products, or otherwise engaging in commercial activities other than those expressly permitted by DPS or the State of New Mexico.

4. DPS may install software and/or hardware to monitor and record all IT resources usage, including email and web site visits. DPS retains the right to record or inspect any and all files stored on DPS systems.

5. Non-business related file downloads will not be permitted unless specifically authorized in writing by the Chief Security Officer (CSO) or the Chief Information Officer (CIO) or their designee. A written request must be submitted to the CSO or CIO.

6. Session activity

   a. All users shall log off or lock their workstations at the end of their work period.

   b. All profiles on all computers that are connected to the DPS network shall employ a locking screensaver that shall be activated after ten (10) minutes of inactivity.

   c. Unless special permission has been granted, users shall not have multiple simultaneous sessions to the DPS network.

   d. Users shall not leave their workstations unattended and unsecured (They must be locked or logged off).

7. Users shall not access or attempt to access IT resources for which they do not have explicit authorization.

8. Users shall not use State of New Mexico or DPS IT resources to override or circumvent any security mechanism belonging to any government agency, organization, or company; except with written permission of the DPS CSO or designee.

9. Users shall not use DPS IT resources for illegal activity, gambling, or to intentionally violate the laws or regulations of the United States, any state or local jurisdiction, or any other nation.

10. Diagnostic or other test hardware and software that can bypass system security shall be used only by authorized personnel for testing, auditing, or development purposes.

11. Employees shall not manipulate or alter any software running on department-owned mobile, desktop, or handheld computers.

K. Internet Use – Occasional and incidental personal use of DPS's Internet access is allowed subject to limitations.

1. Personal use of the Internet shall not materially interfere with the use of DPS IT resources by any State of New Mexico agency.

2. Personal use of the Internet shall not burden DPS with any additional costs.

3. Personal use of the Internet shall not interfere with a user's employment duties or other obligations to the State of New Mexico.

4. Personal use of the Internet shall not include any of the following activities:

   a. Uploading or transferring software, which is owned by or licensed to DPS, out of DPS's control.

   b. Releasing confidential or sensitive information to unauthorized individuals.

   c. Downloading executable software unless it is required to complete a user's job responsibilities.

   d. Downloading or distributing pirated software or data. Distribution of music or video files in any format that is not for DPS business is also forbidden

   e. Deliberately propagating malicious code.

   f. Intentionally disabling or overloading any computer system or network or intentionally circumventing any system intended to protect the privacy and/or security of DPS IT resources.

   g. Using dial-up technology to connect to the Internet without explicit authorization in writing by the State CIO or CSO.

   h. Accessing, storing, displaying, distributing, editing, or recording explicit, extremist, or potentially embarrassing materials. Exemptions to this policy are covered in 1.12.10.9 (I) NMAC.

   i. Soliciting for any business or be associated with any for-profit outside business activity that is unrelated to DPS business.

L. WLAN Use

1. Users shall not connect any un-approved Wireless LAN hardware to DPS IT resources.

2. All DPS laptops, workstations, and servers that are equipped with WLAN hardware shall have their *ad hoc* modes disabled.

M. Removable Storage

1. Removable storage shall not be used without the knowledge and authorization of the CSO.

2. CJIS data or other forms of information that could compromise confidentiality shall not be stored on any form of removable storage.

3. All removable storage that is intended to be discarded or distributed outside of DPS or between intra-agency divisions with different security levels must be given to ITP for media sanitation.

N. Personal Digital Assistants (PDAs)

1. All PDAs that are used to store protected information shall be protected with a password or PIN.

2. All PDAs shall follow the policies stated in section C (WLAN use) and shall meet DPS requirements for WLAN encryption.

3. Only authorized PDAs shall be used on DPS IT resources.

4. DPS-authorized PDAs shall not be used on non-DPS IT resources, including home computers.

5. Unauthorized software and accessories shall not be used or installed on DPS-authorized PDAs.

O. Personal Computing Equipment

1. Employees shall not bring personal computers, peripherals, or software into DPS facilities without prior authorization of the DPS CIO.

2. No protected information shall be stored on any device that is not approved for storage of such information. This includes approved personal devices that are used for remote access.

P. Privacy

1. DPS computer and communications systems are not intended for, and shall not be used for the exercise of the participants' right to free speech.

2. DPS retains the right to remove from its information systems any material it views as offensive, potentially illegal or embarrassing; this includes inflammatory, defamatory, harassing, or disruptive communications.

3. Users of DPS information systems have no expectation of privacy on any medium, including, but not limited to file servers or any form of outbound Internet communication.

Q. Media

1. All storage media that are intended for re-use by either another entity or by another section of DPS that has different security access shall be sanitized prior to re-

distribution. This sanitization shall be approved by the DPS CSO and shall include a multiple pass DoD-approved data wiping program.

2. When no longer usable, all media (including tapes, printer ribbons, hard copies, and removable storage) used to process protected information shall be destroyed (methods may include but are not limited to shredding, incineration, or degaussing) considering which method is appropriate and cost-effective.

7.0 ATTACHMENTS

NONE

8.0 APPROVAL

APPROVED BY: s/ Gorden E. Eden Jr. DATE: March 7, 2011
DPS Cabinet Secretary